12-1-2009

Information Security Disclosure: A Case Study

I Rosewall
Deakin University

M J. Warren
Deakin University

DOI: 10.4225/75/57b401d430de9
7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009

Information Security Disclosure: A Case Study

I. Rosewall and M. J. Warren
School of Information Systens
Deakin Universtiy
Melbourne, Australia

Abstract

New social networking systems such as Facebook are an ever evolving and developing means of social interaction, which is not only being used to disseminate information to family, friends and colleagues but as a way of meeting and interacting with "strangers" through the advent of a large number of social applications. This paper will focus upon the impact of Generation F - the Facebook Generation and their attitudes to security. The paper will be based around discussing the findings of a major UK case study and the implications that this has. The case study identifies 51 recommendations to improve the situation of data security within the military of the UK. These recommendations will be the data for the analysis and will form an overview of the case study's point of view as regards the younger generation and data security. This paper will suggest another interpretation of the results supplied by Burton.

Keywords

Security, Information disclosure, information society

INTRODUCTION

We live in a very different society compared to ten years ago, the Internet and related Information Systems has impacted all developed societies. *"The experience of growing up online will profoundly shape the workplace expectations of "Generation F" – the Facebook Generation. At a minimum, they'll expect the social environment of work to reflect the social context of the Web"* (Wall Street Journal, 2009).

Other key issues with Generation F (or Generation Y, Also called Echo Boomers, or the Millennium Generation, 1979 - 2000) is the expectation that "*their workplace will reflect that of their social lives and that to challenge the 'process' is something that should be achieved"* (Wall Street Journal, 2009). "*Generation Y are 60 million strong, and they have grown up in a more media-saturated and brand-conscious world than any of their predecessors. However, access to information is perhaps the biggest difference between Gen Y and their predecessors. The first generation to grow up with the Internet, They have email accounts, cell phones and access to a dizzying array of fragmented media outlets. As they continue to enter their 20s, Gen Y will soon be an economic force to be reckoned with" (*McCrindle, 2008).

The differing outlook of this generation has been blamed for the decline in data security within the UK military. On the 24th January, 2008 the UK Secretary of State announced to the House of Commons that he had Invited Sir Edmund Burton to undertake a full Investigation into the Ministry of Defences (MOD's) protection of it's personal data after the theft of a laptop which contained 600,000 unencrypted personal records, in Birmingham on the 9/10 January 2008. The outcome of the investigation was the report "Loss of MOD Personal Data" was presented to the UK's Permanent Under Secretary MOD on the 30th April 2008 (Burton, 2008). This paper will look at the impact of Generation F and focus upon the `Loss of MOD Personal Data` Case Study to highlight future security trends.

BACKGROUND DISCUSSION

In November 2007 Her Majesty's Revenue and Customs (HRMC) (This department deals, amongst other things, with Child Benefit payments to families in the UK), lost 2 CD's containing (BBC 2007):

- 7.25 million claimants;
- 15.5 million children, including some who no longer qualify but whose family is claiming for a younger child;
- 2.25 million 'alternative payees' such as partners or carers;
- 3,000 'appointees' who claim the benefit under court instructions ;
- 12,500 agents who claim the benefit on behalf of a third party.

The discs contained 25 million records. These included the names, addresses, dates of birth, National Insurance numbers and, where relevant, bank and building society details.

Following this incident, the British Prime Minister Gordon Brown, commissioned a review on into Data Handling procedures within government. In June 2008 the final report was published `Data Handling Procedures in Government:

Final Report` with key recommendations (Cabinet Office, 2008). These measures were to be adopted by all UK Government Departments.

On the evening of 9/10th January 2008 a laptop was stolen from a Royal Naval recruitment Officers car in Birmingham, England. It contained 600,000 unencrypted personal records of potential recruits and circa 400,000 next of kin and referee records. On the 11th January the Incident was reported to Ministers of the British Government. It had not been reported that the Information was unencrypted until the 14th January. On the 24th January the Secretary of State announced to the commons that he had Invited Sir Edmund Burton to undertake a full Investigation (BBC 2008).

The Burton Report was tasked with reviewing the MOD's protection of its personal data after the theft of a laptop in Birmingham on the 9/10 January 2008. Burton's review was carried out using the terms of reference set out by the UK Secretary of Defence (Burton, 2008) which stated: *"To establish the exact circumstances and events that led to the loss by MOD of personal data; to examine the adequacy of the steps taken to prevent any recurrence, and of MOD policy, practise and management arrangements in respect of the protection of personal data more generally; to make recommendations; and to report to MOD's permanent secretary not later than 30th April 2008".*

The following section of this paper will discuss and analyse the findings and recommendations of this report with particular focus on the categories that Burton has assigned certain problems to.

ANALYSIS OF REPORT INTO THE LOSS OF MOD PERSONAL DATA

The final report "Report into the loss of MOD Personal Data" (April 2008) was delivered to the Permanent Under Secretary MOD on the 30th April 2008.

The preamble to the main report admits that the MOD had been less than proactive in its protection of Data. The general findings indicate that there is *"little awareness of the current, real, threat to information...."* and that *"a major security incident had been inevitable"* several reasons were postulated as to the progression of this situation, these included; not treating Information, Knowledge and data as operational assets; Risk to information not being managed at executive board level and very limited understanding of the data protection act.

As part of the Investigation carried out by this report was to highlight progression of the MOD's departments through the preceding three years. This Investigation found that 42 of the 76 recommendations had been implemented prior to the theft of the laptop in Birmingham. The remaining 34 were to be integrated with the Cabinet report and the Burton report on its completion.

The report stated that 2007 losses or theft of laptops within the MOD totalled 130 (0.4%) out of 35,000 this was deemed to be in line with the 1-2% Industry had suffered, and as such, it would appear, there was no need for further Investigation. With regard to other storage devices such as USB's external hard drives and PDA's there were no firm statistics as to how many the MOD owned and for that matter, how many were owned by individuals, or what unencrypted data was stored on these devices.

The report was also quite damning of the fact that the recording of thefts and losses was 'unsatisfactory' *"despite there being a comprehensive policy for alert, warning and response in Joint Service Publications (**JSPs**) 541".* (MOD 2004) This being the case the loss of personal data could be more severe than first thought.
Part one of the Burton report sought to investigate *"The main circumstances and events that led to the loss by MOD of Personal Data on 9th January 2008."* Burton concentrated his efforts here to the data loss as opposed to the laptop loss. The data lost, he concluded, was the product of non compliance to the security orders given in various instructions over a period of time. The question of encryption rather than physical security would appear to be the focus of this report. Little or no mention of the physical security of the four Laptops stolen from various MOD personnel over a period of four years seems to be warranted. The report also highlights that one of the stolen laptops was not even reported which begs the question how many more would fit into this category? It would also appear that only one (The most recent) of those responsible for the physical security of the Laptops is subject to disciplinary proceedings. This in itself questions whether JSP's are actually being implemented.

Part two of the report investigates "MOD protection and Management of Personal Data" Burton begins this section "*The major impact of this event* (Birmingham 2008) *was an inevitable outcome of a series of failings in governance, process and leadership"* He describes six areas of major concern (Burton 2008):

Cultural Changes (The Facebook Generation)
Burton accepts that there has been a significant change within the culture whereby we now live in an environment where *"the rapid and often uninhibited exchange of Information is the norm"* A situation where this, behaviour in the

workplace, could be devastating. Burton suggests that this behaviour should be *"tempered by common sense and sound judgement"* he also rules out the possibility of returning to the paper systems and thinking of fifteen years ago, arguing that cannot be considered practical in the modern working environment.

New ways of working
In order to illustrate this point the report cites the Human Resources Management System (HRMS) and explains that this system is an example of capitalising on new technologies and the shift in cultural developments. The risk management of this *"better access to personal data"* as yet, has not been recognised at 'Board' level. This highlights generic problems within the military, in that they see this as an add on. Bishop (2003) informs us that: *"Security is not an add-on or merely an operational concept, it is a property that must be designed and built into every system."* Perhaps we could add here "from the outset".

Decline in Security
Anecdotal evidence would suggest that these modern working practises has produced a decline in the security at department level and more disturbingly at a personal level. Burton goes on to say that *".. the younger generation of MOD staff are not inculcated with the same culture of protecting Information as their counterparts from previous generations."* Alluding of course, to the 'cold war' era, where Information security was of paramount importance.

"Security is a chain; it's only as secure as the weakest link." (Schneier, 2000).

Resourcing Security
As is the trend in governments to make themselves cost effective, cuts in staff are inevitable, thus making the resourcing of security difficult. Burton cites the need for *"accreditation, audit and compliance"* and yet the department has *"a significant shortage of accreditors who are crucial to the validation of security measures in ICT systems"* Interestingly there is no mention here of security training even though many authors highlight it's need, Michael E. Whitman (2003) suggests that "*Information security continues to be ignored by top managers, middle managers, and employees alike. The result of this neglect is that organizational systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than is necessary".*

Accounting for Computers and USB Devices
In this very brief section Burton makes us aware that the *"accounting for Laptops, PDA's and USB devices and the reporting of losses, is poor....."* He argues that this can cause ineffective management of the security of the data and the devices on which data is stored, although there is a set procedure for this (MOD 2004).

'Need to Know' versus 'Need to Share'
The report addresses the issue of the MOD philosophy of "Need to Know" against the modern working practises of "Need to Share" a conflict that needs to be resolved as a matter of urgency. Burton holds the view that it would be "impractical" to return to the 'Cold War' scenario, however the modern position of "Need to Share" leads to *"unacceptable vulnerabilities"*. Accepting this situation means that working practises within the MOD need to be reviewed without ignoring the benefits of the new emerging technologies and yet still being vigilant with regards to Information security.

Burton, on completion of this report, gave a total of 51 recommendations, the analysis of which will form the main thrust of this paper. In the process of forming the 51 recommendations for this report Burton identified areas of concern within the MOD which reflect the current social environment in which we live and the potential dangers that this "Facebook Generation" can inflict upon today's modern military.
In the interest of brevity this paper will concentrate on the recommendations that allude to the 'People' section and examine whether, at least some of them, could be expressed in a slightly different manner, they include (Burton, 2008):
Recommendation 2: MOD to ensure that all employees and contractors understand what key information and documents must be maintained as records, and to highlight consequences of failing to do so.

Recommendation 9: MOD to ensure that individual and corporate responsibilities under DPA 1998 are understood and complied with.

Recommendation 23: Detailed accountabilities for Data Protection across the Department to be clearly articulated.

Recommendation 30: MOD to define the full scope of responsibilities for the Departmental Chief Information Officer functions.

Recommendation 31: MOD to reinforce the authority of the MOD SIRO to act on behalf of the Defence Operating Board in respect of information risk.

Recommendation 38: MOD to review and formalise a coherent system of censure and punishment for those who lose or compromise personal data, where the level of punishment reflects the scale and seriousness of the loss; seeking to apply this equitably, regardless of whether the individual responsible is military or civilian, government employee or contractor.

Recommendation 41: MOD to implement the principle of storing and handling only the minimum amount of personal data required to carry out core business.

Recommendation 42: MOD to implement a challenge process, both in terms of deciding whether personal data should be kept in the first place, and then on whether it should be accessed and downloaded on to removable media devices.

Recommendation 46: Arrangements to be made for senior leaders and managers to receive a comprehensive briefing on the current threat picture and for formal updates at appropriate intervals.

Recommendation 47: The current threat picture to be clearly and briefly set out to other relevant MOD staff, as a matter of urgency, with formal updates at appropriate intervals.

Recommendation 48: Security Doctrine and Operational Security work to be at the heart of the campaign for raising awareness of the importance of information and data to the Department and the significance of protection measures.

ANALYSIS (CONCEPTUAL MODEL)

This section of the paper seeks to investigate, in detail, the recommendations in the Burton report discussed earlier. Edmund Burton gave us 51 recommendations which he has broken down into 5 distinct sections. He had categorised each of his recommendations to fit into (Burton, 2008):

Processes	31 recommendations which equates to 61% of the overall recommendations.
People	11 recommendations which equates to 21%
Training and Education	5 recommendations which equates to10%
Technology	3 recommendations which equates to 6%
Others	1 recommendation which equates to 2%

Figure 1 is a graphical representation of this breakdown and highlights breakdown of recommendations.

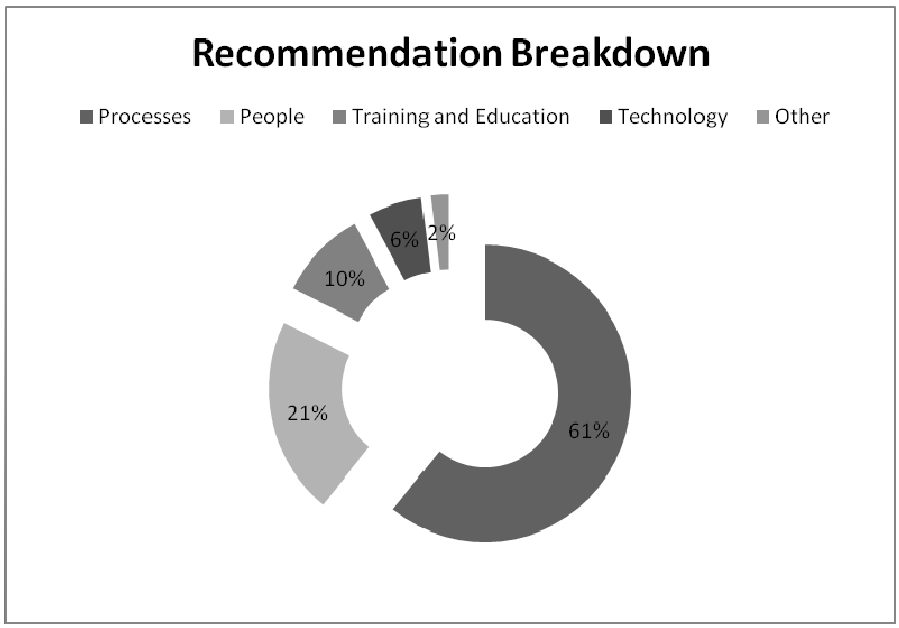

Figure 1 - Breakdown of Burton Recommendations

As has been stated in the previous section we will concentrate on the recommendations that allude to the 'People' section and examine whether, at least some of them, could be expressed in a slightly different manner. Figure 2 shows the current relativity of the Burton report recommendations.

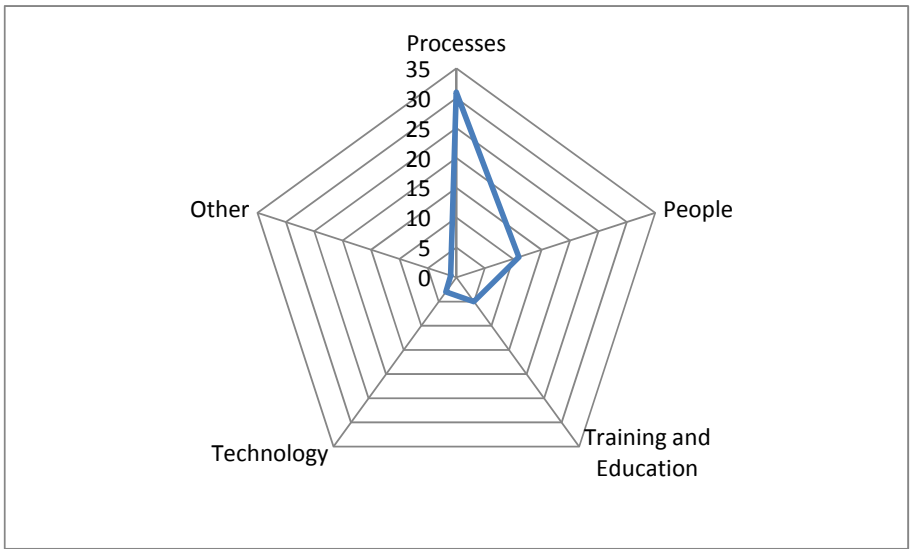

Figure 2 - Focus of Burton Recommendations

Figure 2 shows a graphical representation of the relationship between the different categories of the recommendations. It depicts the situation before the analysis and shows a high bias towards the 'process' section of the recommendations. As this report was written by civil servants *for* civil servants it will come as no surprise that this is the case. After analysis of the recommendations we will review these categories to see if they can be illustrated in any other way.

DETAILED ANALYSIS OF KEY RECOMMENDATIONS

These recommendation categories are open to interpretation and as such bears further investigation. This section examines these recommendations in a little more detail and suggests that there is an alternative to that that has been offered by Burton (Burton, 2008):

Recommendation 2: MOD to ensure that all employees and contractors understand what key information and documents must be maintained as records, and to highlight consequences of failing to do so.

This recommendation refers to the apparent lack of understanding of requirements between the contractor and the MOD staff with regards to encryption of the laptops. The confusion is understandable when you consider that Information Security was a new field for most involved and the confusing array of instructions, re-writes and interpretation of these documents could not have helped the situation. This recommendation could have easily sat within the process section as well as the people section. A furtive mention of personal security was mentioned as a codicil to what Burton believed to be the salient point. "*.... the user was in clear breach of physical security rules*" unlike the rest of this report which states quite clearly which order or instruction was broken, this comment was left uncited.

Recommendation 9: MOD to ensure that individual and corporate responsibilities under DPA 1998 are understood and complied with.

DPA 1998, amongst other directives, states that the MOD should; "*Identify and record the purpose for which personal data are being processed and conduct regular checks to ensure that personal data is safeguarded appropriately and is held for legitimate business reasons.*" This recommendation should sit squarely beside recommendation 41(see below) The question of why data is being held, and is continued to be held, should be a matter of some concern for the MOD as further writings in this paper will highlight, data is being held even after its usefulness has little relevance to current 'business' practises. It could be argued that this addresses the data and responsibilities more directly than it does the 'people' title that it has been given.

Recommendation 23: Detailed accountabilities for Data Protection across the Department to be clearly articulated.

Again there seems to be a tendency to highlight the process within the people environment as opposed to the people in the people environment. Continued use of the word accountability as opposed to awareness, the 'stick' and little evidence of the 'carrot'. However Burton does go on to say: *"Beyond the expert community there is little evidence of awareness of the Data Protection Act or its implications for the chain of command*" and admits that there is a *"need for appropriate training."* Along with this data protection training there is also a 'need' for personal security training at all levels within the MOD, Which seems, on the surface, to have been overlooked in this report which would appear to focus more closely on the 'Personal data' as opposed to 'personal security of that data'. *The foundation of any computer security education or training should provide the student with the motivation for the field, i.e. why do we worry about computer security, why is there a problem, and what are the potential consequences*

Recommendation 30: MOD to define the full scope of responsibilities for the Departmental Chief Information Officer functions.
A recent Cabinet Office directive has advised that there should exist a position of Senior Information Risk Officer (SIRO) which should sit at board level. Although this person should be an "executive familiar with Information risks and the organisations response, may also be the CIO....." It still does not address the issues that exist within the MOD at the 'coal face', again the inference here is that security issues should be accountable to an individual rather than an issue which should address the "Facebook Generation" however, for the purposes of this paper it is fair to allow this to reside in the people section.

Recommendation 31: MOD to reinforce the authority of the MOD SIRO to act on behalf of the Defence Operating Board in respect of information risk.

This is purely and administrative recommendation and as such requires no comment

Recommendation 38: MOD to review and formalise a coherent system of censure and punishment for those who lose or compromise personal data, where the level of punishment reflects the scale and seriousness of the loss; seeking to apply this equitably, regardless of whether the individual responsible is military or civilian, government employee or contractor.

This is the first recommendation that addresses the human element of security. It would appear, on first sight, to be fraught with problems. If this recommendation was aimed, solely at the MOD, it would be a little less problematic than trying to encompass 'civilians' as it proposes to do. If it *were* dealing with MOD personnel only, military law would be prevalent and there would probably exist, a comparable offense which could be used as a benchmark, fines, loss of seniority for promotion or even confinement dependant on severity. However the question of equity and enforcement where the offender is a civilian could cause the MOD significant problems. If civilians are to be treated differently then the MOD (no longer enjoying crown immunity) could offer itself up for another round of legal proceedings last experienced when women who fell pregnant sued the MOD. If on the other hand the censure and punishment is consummate with the civilian perspective then where does that leave the MOD on its benchmarking of offenses.

Recommendation 41: MOD to implement the principle of storing and handling only the minimum amount of personal data required to carry out core business.

As with all Public Sector departments the perceived need to capture as much information as possible 'just in case' is prevalent in the minds of those who work within the HQ areas. It is interesting that in the glossary that accompanies this report there is a definition of Information Assurance, Information Security and Information Security Management System (ISMS) but not one for Information! What exactly is being stored, what is relevant, what is data and what is Information. Should this recommendation be in the people section at all or would it sit better in the process section or indeed in training and education?

Recommendation 42: MOD to implement a challenge process, both in terms of deciding whether personal data should be kept in the first place, and then on whether it should be accessed and downloaded on to removable media devices.

The comments made above (41) could equally apply here. However this recommendation goes some way to try to alleviate the problems caused by holding excessive amounts of data for the 'what if' scenario. It addresses the issues made in previous sections by asking the 'why do you need it' question rather than 'how can we secure it better' question. Whether this sits within the parameter of the people section is questionable.

Recommendation 46: Arrangements to be made for senior leaders and managers to receive a comprehensive briefing on the current threat picture and for formal updates at appropriate intervals.

Recommendation 47: The current threat picture to be clearly and briefly set out to other relevant MOD staff, as a matter of urgency, with formal updates at appropriate intervals.

Recommendations 46 and 47 deal with the same area, only the target audience differs and once again we see what should be a clear 'person' recommendation drifting towards the 'process', 'formal updates' and 'threat pictures' moves the perspective towards the management of Information flow as opposed to the management of the staff who deal with the Information, Burton himself states that "....for instance, during the Cold War, each and every person involved in handling crypto material was aware of the very damaging consequences should it be compromised. There is no evidence that a similar mentality existed as regards personal data (at least not before 9 January 2008)." This would indicate that an inbred personal security was needed comparable to the 'cold war' mentality, rather than lengthy 'comprehensive briefings' and 'formal updates'.

Recommendation 48: Security Doctrine and Operational Security work to be at the heart of the campaign for raising awareness of the importance of information and data to the Department and the significance of protection measures.

This is the only recommendation outside of the section on Training and Education section, that focuses on the personal security of the staff involved be they, MOD staff or, civilian. It looks closely at the lives of the staff on operations, with the additional stresses that that would involve and, with the more relaxed atmosphere of working under normal circumstances. There is mention of a needs analysis for all staff members that we hope will address 'personal security' as opposed to 'personal data security' a very different issue.

DISCUSSION

If we are to accept that several of the recommendations do not sit comfortably in the area in which they have been put, then the diagram shown in figure 2 will change. As with most Public Sector organisations the tendency is to look, and concentrate on the process rather than the environment in which it sits and, the environment will always be complex when we are dealing with a human interface (People) Figure 3 shows the same recommendation but viewing the report after the analysis has taken place.

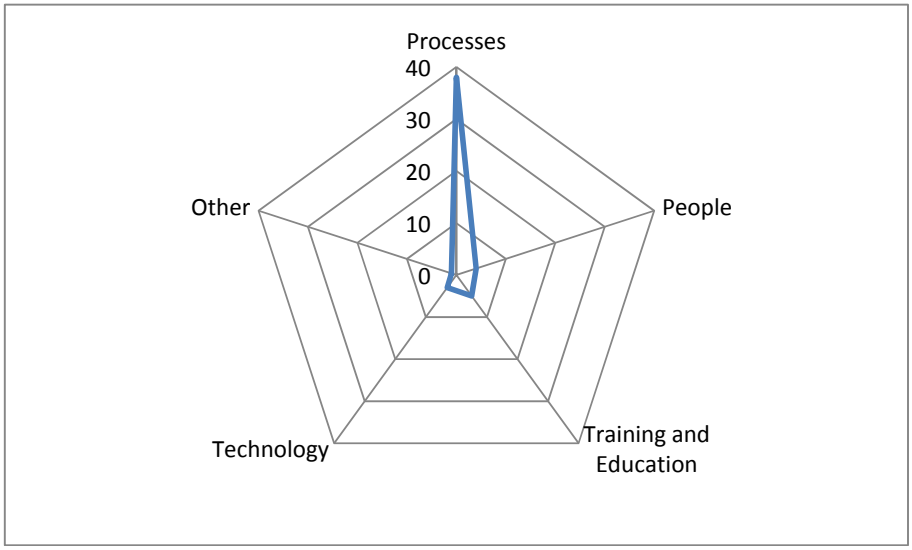

Figure 3- Comparison of Bias

Figure 3 shows a shift from the 'people' section reflecting the analysis, to the 'processes' section. This paper has looked at 11 of the Burton Report recommendations in some detail and has compared this 'People' section to what is generally perceived to be the 'fault' of personnel. Recommendation 30, 31, 38 and 48 would appear to sit quite legitimately in this section, whereas 7 others could easily be moved to the section 'Processes'. There seems to be a tendency to highlight the process within the people environment as opposed to the people in the people environment. Continued use of the word accountability as opposed to awareness would appear to reinforce this position. The alarming figures that appear in the report add credence to the general belief that the MOD as with most Public Sector departments, feel that they have the need to capture as much information as possible and store for 'future reference' further emphasising this 'process' mentality.

Figure 3 also illustrates where the bias exists after the suggested alterations from the analysis conducted above. It reflects where recommendations 30, 31,38 and 48 have stayed in their original section (People) and no less than seven other recommendations 2, 9, 23, 41, 42, 46 and 47 have been moved to the 'Processes' section where the authors believes that they should reside.

CONCLUSION

After close analysis of this document it was revealed that the theft that sparked this report was merely the tip of the iceberg. Several thefts within government departments led UK Ministers to question the very fabric of their data handling capabilities. The Burton report has identified several issues outside of its remit, begging the question, has the investigation gone far enough? Was the remit for this report too restrictive? Further research into these questions bares thought.

This paper has only scratched the surface of Burton's report there are several areas that need further examination an example of which is, in the glossary that accompanies this report there is a definition of Information Assurance, Information Security and Information Security Management System (ISMS) but not one for data, information or knowledge. The staggering amount of data that was stolen highlights the need to re-evaluate the way that the MOD and for that matter, other public sectors store, use and abuse data and information. There are several mentions of the 'cold war' within the main report. Which is viewed with some distain, and yet it favours this attitude to that of the 'Facebook' generation which in itself offers a whole new outlook on the work environment and could open up a plethora of problems for UK government departments which rely on the discretion of its employees.

Burton's report offers reasons and recommendations for the future of the MOD's security of data. It does not examine the mentality of the generations which are soon to be the 'Captains of this Industry' further research is required to look at the implications of this 'web 2' generation and the concept of personal and organisational security in today's military. This further research would be enhanced by hard data relating to the 'other' generations which could then be used as a comparison to fully understand if the current problems are attached to just one generation or, has there been a decline in general security attitudes towards data security over several generations.

REFERENCES

BBC (2007) UK's families put on fraud alert, URL: http://news.bbc.co.uk/2/hi/7103566.stm, Accessed 10th September, 2009.

BBC (2008) MoD 'Facebook generation' warning, URL: http://news.bbc.co.uk/2/hi/uk_news/politics/7473818.stm, Accessed 5th September, 2009.

Bishop,M, (2003) "What Is Computer Security?," IEEE Security and Privacy, vol. 1, no. 1, pp. 67-69, Jan. 2003,

Burton, E (2008) Report into the Loss of MOD Personal Data, Minsitry of Defence, UK, Report accessible via: http://www.mod.uk/NR/rdonlyres/3E756D20-E762-4FC1-BAB0-08C68FDC2383/0/burton_review_rpt20080430.pdf, Accessed 15th September, 2009.

Cabinet Office (2008) Data Handling Procedures in Government: Final Report, UK Government, Report accessible via: http://www.cabinetoffice.gov.uk/media/65948/dhr080625.pdf, Accessed 15th September, 2009.

McCrindle M, (2008) The ABC of XYZ: Generational Diversity at Work. M Crindle Research Pty Ltd http://www.quayappointments.com.au/email/040213/images/generational_diversity_at_work.pdf, Accessed 20th October 2009

Michael E. Whitman (2003), Enemy at the gate: threats to information security. Communications of the ACM ,Volume 46, Number 8, Pages 91-95

Ministry of Defence (2004) JSP (Joint Service Publication) 541 - MOD Information Security Alert Warning and Response Policy Manual, UK.

Schneier B, (2000) Secrets & Lies: Digital Security in a Networked World, 1st edition John Wiley & Sons, Inc. New York, NY, USA

Wall Street Journal (2009) Gary Hamel's Blog: The Facebook Generation vs. the Fortune 500; 24th March, URL: http://blogs.wsj.com/management/2009/03/24/the-facebook-generation-vs-the-fortune-500, Accessed 15th September, 2009.

COPYRIGHT